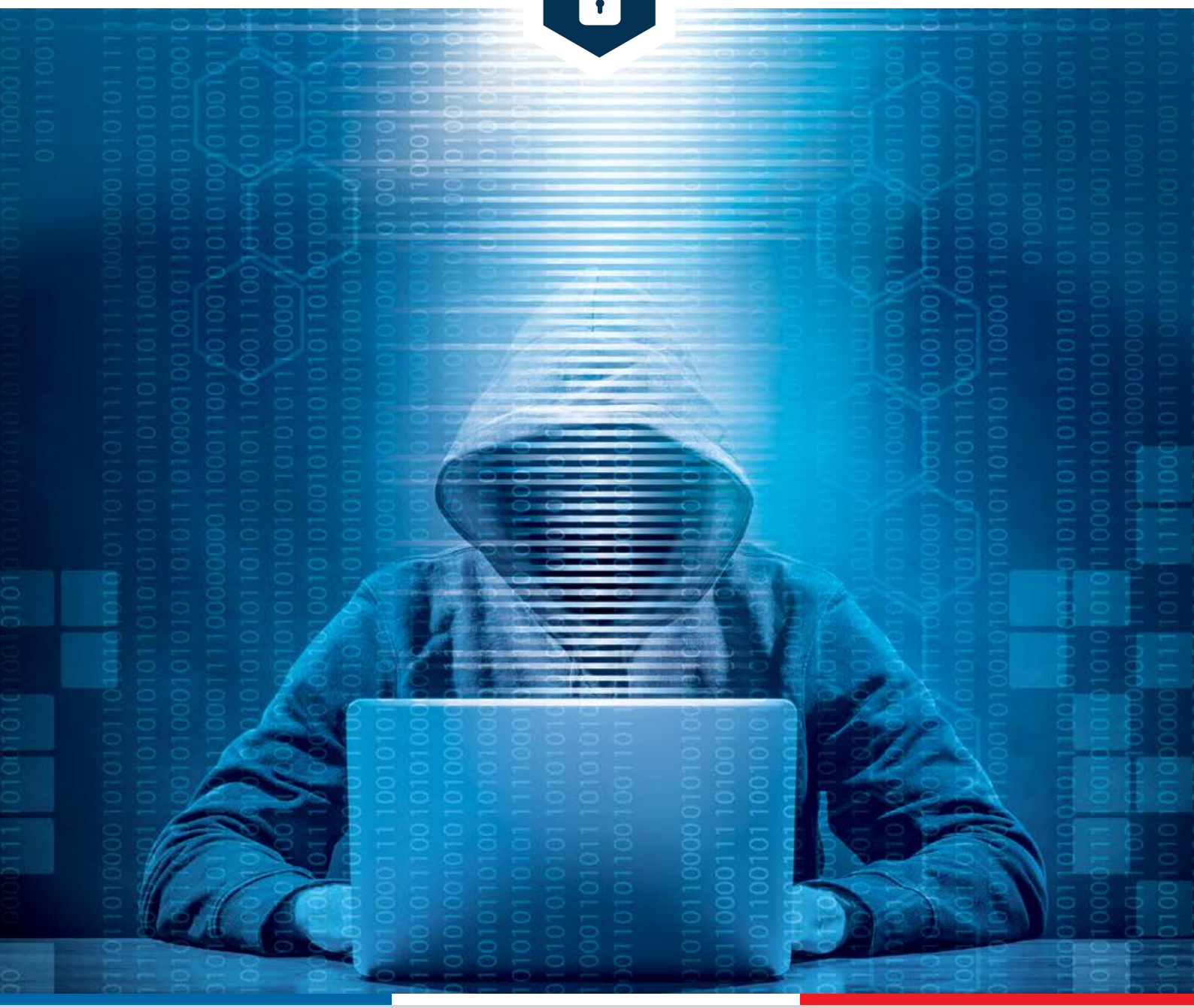
CYBERSECURITY

[PROTECT - RESPOND - ANALYSE]



GICAT

FRENCH ASSOCIATION OF LAND AND
AIR-LAND DEFENCE AND SECURITY INDUSTRIES

IN PARTNERSHIP WITH:

HEXATRUST

CYBERSECURITY & DIGITAL TRUST

EDITORIAL
ANSSI

FRENCH CYBERSECURITY AGENCY

Our activities are focused on new information and communication technologies that can involve both daily life digital exchanges, and operations of the most critical systems. Whilst these technologies can significantly improve the effectiveness of our systems, they also render them more vulnerable. The number of cyber attacks is growing daily and these attacks are becoming increasingly sophisticated.

In this ever-changing context, ANSSI, the French cybersecurity agency is working with the cybersecurity field actors to develop and promote an industrial offer capable of effectively dealing with all current and future threats.

The French offer incorporates a strong network of innovative companies with internationally recognised expertise and knowledge. This offer is known for the quality, diversity and complementarity of its products and services, and can cover all the needs of French and international companies and administrative organizations.

ANSSI welcomes and supports the work of the French driven industrial cybersecurity branch through a number of recent initiatives including the launch of the France Cybersecurity label, the joint attendance of government and industry representatives to international events, and the structuring of corporate associations. This brochure that showcases several French industrial flagships is another example of the dynamism of this field.

Guillaume Poupard
Director General

FOREWORD
GICAT / HEXATRUST

IT security threats are a major concern in today's world. Everyday attacks and their consequences are discovered on a daily basis, whether in terms of personal data breaches affecting individuals or the leakage of sensitive information inside companies and administrations.

To counter these threats, GICAT (Groupement des Industries de Défense et de Sécurité Terrestres et Aéroterrestres, French land defence and security industry association) and HEXATRUST (Cybersecurity & Digital Trust Alliance) have decided to join forces, creating a partnership based on the complementary nature of their organisations. Founded by innovative French SMEs and start-ups at the forefront in cybersecurity, HEXATRUST reflects their expertise and know-how in their fields. GICAT reinforces this industrial ecosystem and offers support for exportation through its participation in international trade fairs and prospecting missions and related services.

This Cybersecurity Capabilities brochure presents a network of French companies seeking to develop their international business.

They are all recognised for their know-how and ability to innovate in the fields of Information Security Systems, Digital Trust and Cybersecurity. Some have received the FRANCE CYBERSECURITY LABEL, which represents an added guarantee of security and quality.

INTRODUCTION

CYBERSECURITY

Cybersecurity is one of the major priorities of the 21st century and an issue that reaches across borders in our highly connected world. Some 15 billion objects are now connected, and this will reach 50 billion by 2020.

Cybersecurity is an extremely vast field. It concerns governance sectors (defence, national security, and public administrations), vital infrastructures (energy, transport, health care, etc.), the private sector (industries, banks, businesses, services, etc.) and the population at large.

This threat can put any entity at risk, regardless of its sector, size or activity. It is a constant and diffuse threat that can come in many forms: obfuscation, theft, monitoring, abuse and usurpation of rights, data corruption, etc. Industrial systems that are interconnected with networks are particularly vulnerable targets. At the global level, the financial stakes represent billions of euros.

FRENCH EXPERTISE

France has demonstrated incontestable know-how and expertise in cybersecurity, including aspects such as encryption, smart cards, biometrics, authentication and electromagnetic radiation. French manufacturers have developed and continue to upgrade their products in all of the sub-sectors making up the broad spectrum of cybersecurity.

THE BROCHURE

The purpose of this brochure is to present a range of cybersecurity capabilities based on possible solutions provided by the products and services of the companies belonging to the GICAT security cluster and the HEXATRUST alliance. These solutions are independent but often complementary and can be selected globally to meet a specific requirement.

In collaboration with research institutes, the companies presented in this brochure, including innovative software publishers, offer a range of products adapted to every operational context and regulatory constraint in the world.

THE CYBERSECURITY CYCLE

The cybersecurity cycle can be broken down into three components:
"PREVENTION AND PROTECTION"; "DETECTION AND RESPONSE"; "INVESTIGATION AND RESILIENCE".

1 / The "PREVENTION AND PROTECTION" component precedes an incident and lasts throughout the system's entire lifespan.

This includes aspects such as:
- anticipating and foreseeing threats and vulnerabilities and identifying the risks they represent
- defining architectures and procedures
- installing, configuring and maintaining resources in proper working order
- training personnel

This component concerns all products and solutions used to prevent and counter incidents and losses on an infrastructure.

2 / The "DETECTION AND RESPONSE" component allows attacks to be detected and contained.

The goal is:
- to detect incidents and losses
- to collect and analyse data flows and behaviours on systems in order to detect an incident if it has not already been reported
- to trigger an adequate response in order to contain the incident

This component concerns all products and solutions used to detect and block incidents and losses on an infrastructure.

3 / The "INVESTIGATION AND RESILIENCE" component follows an incident.

The goals of this phase are:
- to analyse the incident in order to keep it from happening again
- to gather proof in the event of system abuse
- to enable continuity of service

This component concerns all products and solutions used to minimise the damage resulting from incidents and losses, analyse what happened, and restore the initial condition as necessary.

FUNCTIONAL BREAKDOWN

Protecting and securing information requires setting up tools, processes and organisation systems that can meet defined availability, confidentiality, integrity and traceability objectives. These actions are broken down into two distinct scopes:

• INFRASTRUCTURE PROTECTION for the physical means and the network. This consists in securing the buildings, machines and networks by setting up firewall and antivirus technologies and intrusion detection solutions.

• INFOSTRUCTURE PROTECTION or Information Protection consists in securing the data and the applications that use them. This scope covers both data security and application security.

The functional breakdown of "cybersecurity" is as follows:

IDENTIFICATION AND AUTHENTICATION

Controlling access to a site is an essential security measure which ensures the physical protection of the information and information system and the authenticity of the hardware.

To provide these guarantees, these measures must first include means capable of physically recognising a person or device; this is the identification aspect. They must then be capable of verifying their authenticity; this is the authentication aspect.

In the digital world, as in the physical world, it is essential to confirm people's identity and authenticity using means such as physical identity, biometrics and cryptography, etc.

IDENTITY AND ACCESS MANAGEMENT

In our interconnected world, an organisation's information assets are a vital resource. The disclosure of digital information can be a serious blow to an organisation. For any entity that possesses sensitive information, information traceability and imputability of actions are major priorities.

The purpose of an identity and access management system is to control "who has access to what", such that only authorised people or devices have access to the resources (data, information, etc.) they are allowed to access. The processes for requesting or revoking rights of access must be managed continuously and in an audited and controlled manner, in accordance with the security policy.

DATA SECURITY

The loss of data due to an incident, whether voluntary or not, can be catastrophic or even fatal to an entity. The availability of processed information always needs to be taken into account when securing an information system.

It is essential that the confidentiality, integrity and traceability of information be guaranteed, especially through the use of cryptographic means. An electronic signature allows a person to commit to data (non-repudiation) and to vouch for the data's integrity. It is also important to ensure data integrity in the long term and to conserve the legal value of digital proof over time.

Encryption tools are used to manage data confidentiality, both between different people within a company and any time data is shared, exchanged or stored.

INFRASTRUCTURE AND EQUIPMENT SECURITY

An information system's infrastructure is a vital element, and the security of its architecture needs to be ensured by guaranteeing the confidentiality, availability and integrity of every brick that makes up the system.

This is achieved by securing the entire system, i.e., every device and technology, the interconnections and the configuration parameters.

Hidden channels and transmission via interfering signals must also be taken into account to prevent the leakage of sensitive information.

COMMAND AND CONTROL, DECISION SUPPORT

Sensitive infostructures require around-the-clock surveillance, 24-7, in order to detect security incidents affecting the information system.

The tools used for this surveillance need to manage the activity logging for the system's components and analyse the data flows to provide the security teams with information. For better detection of complex attacks, they must also be able to associate related events and provide the appropriate summary reports.

PROVIDING AND COLLECTING INFORMATION

In cyberespace, information is the raw material and represents a vital resource. Controlling information has therefore become a major priority for companies and government agencies.

With the growth of data transfer platforms and social networks, surveillance of these channels is essential.

The diversity and volume of multilingual information exchanged in the digital world means increasingly effective, high-performance tools are needed to collect, analyse and provide relevant information with confirmed value.

INVESTIGATING AND GATHERING PROOF

After a security incident, it is important to investigate what happened in order to take legal action and/or keep this type of event from happening again.

The digital investigation must:

• first, ensure the integrity of the digital proof and that all items of evidence are properly conserved,

• second, analyse this proof which can be complex,

• and lastly, provide an investigation report that can be understood by non-experts in the field.

AUDITING, CONSULTING, OPERATIONS AND TRAINING

Guaranteeing the protection of information assets is of utmost importance. Securing the information system and keeping it secure over time is an action that every entity needs to implement.

Given the complexity and diversity of interconnected technology systems, achieving system security requires experts well-versed in not only information system security, but also every technology used to handle information.

These specialists have the necessary qualifications to contain an incident on the system and respond quickly and effectively in order to limit its impact.

These consultants are able to provide services at every level: governance, control and design/integration.

Every link in the chain of an information system plays a part in its security, and cybersecurity trainings are essential in ensuring infostructure security.

COMPANY INDEX

FUNCTIONAL BREAKDOWN

	Page	Identification and Authentication	Identity and Access Management	Data Security	Infrastructure and Equipment Security	Command and Control, Decision Support	Providing and Collecting Information	Investigating and Gathering Proof	Auditing, Consulting, Operations and Training
AIR LYNX	10				●				
ATOS	11		●	●		●			
BERTIN	12			●	●		●		
BRAINWAVE	13		●	●	●				
COFELY INEO	14			●	●				●
DENYALL	15	●		●					
ERCOM	16	●	●	●					
ILEX	17	●	●						
OPENTRUST	18	●	●	●					
PRIM'X TECHNOLOGIES	19			●					
RISK & CO	20				●			●	●
SURYS	21	●			●		●		
SYSTRAN	22						●	●	
THALES	23	●		●					●
THE GREEN BOW	24			●	●				
TRACIP	25			●				●	●
TRUSTINSOFT	26			●	●			●	
VADE RETRO TECHNOLOGY	27			●	●				
WALLIX	28		●	●				●	

AIR-LYNX

Manufacturer and supplyer of 4G LTE secure private networks dedicated to fixed or nomad professional usage

AIR-LYNX 4G NOMAD AND SECURED NETWORK

AIR-LYNX proposes an innovative solution for a 4G LTE private network featuring the four native communication services PMR (included "Push to Talk", group calls and priority management), video, geopositionning and telephony, required for professional usages. The infrastructure provides a warranted access to the resources and a high data rate transmission.

AIR-LYNX 4G solution is based on recent LTE technology and takes advantage of frequency agility, compact packaging, ease of deployment and international standardization which warrants smooth evolution and long life duration. It incorporates one LTE network kernel (ePC), one or several LTE base stations (eNodeB), servers associated to the four native services and optional gateways required by customer for interoperability purposes. AIR-LYNX can also include in its supply, standard or ruggedized mobile devices as smartphones or tablets which could also be secured, as well as the services required for deployment field engineering.
Fitting well military or public safety applications, it can be supplied for fixed or mobile facilities as well as a transportable version for tactical radio network deployment.

NATIVE SECURITY SERVICES:

- Terminals identification and authentication, mutual authentication between network and terminals
- Users identification and authentication,
- User and terminal identity confidentiality,
- User data confidentiality between terminal and base station (radio channel),
- Signalling data confidentiality and integrity between terminal and network kernel,
- End to end user data confidentiality (optional),
- Built-in event reporting.

CONTACTS:

AIR-LYNX
Immeuble Everest, 1 Avenue de l'Atlantique
91940 LES ULIS - FRANCE
Tel.: +33 (0)9 81 43 46 46
Web site: www.air-lynx.com

Philippe SAENZ
President
Mobile: + 33 (0)6 32 95 03 26
philippe.saenz@air-lynx.com

Atos

Atos manages the entire security process (from consulting to operation) and covers the whole security value chain, from IT to operational technologies.

Atos is a trusted partner, addressing security specialists as well as general management and business managers.

AHPS (Atos High Performance Security) with SIEM (Security Information and Event Management) and CSIRT (Computer Security and Incident Response Team) work together to detect and remediate security issues, while adding value to your activity.

Data protection: sensitive data is pervasive in your organization and in its exchanges with the outside world.
Trustway Proteccio is a general-purpose HSM. It provides hardware protection for keys management and cryptographic operations.
Trustway VPN protects your sensitive networks and all their endpoints against intruders. It ensures the confidentiality and integrity of IP flows.
Globull is an external hard drive with a very high level of security. You can safely carry your sensitive data with you.

Atos has provided the entire IT for the Olympics including all key security services since 2002 and until at least 2024. The Olympics has not had a single business interruption due to an IT security incident in the 12 years we have worked with them—this despite the Games being an extremely rich target for hackers.

Hoox: native mobile security. The Hoox phones are designed to provide you with a high level of security. Controlled communication ports, strong authentication, hardware encryption: the entire phone protects your privacy. Atos integrates Hoox encryption technology and high-performance anti-intrusion protection. The entire safety chain is protected.

Atos' Evidian Identity and access management software protects access to your information system's resources. It considerably simplifies the management of authentications and access rights, and delivers single sign-on for PC, web and mobile. As a result, your users are more productive and comply naturally with your security policy.

Atos Physical Security is an integrated solution that ensures the overall security of major, sensitive sites. Physical security includes access control, video surveillance and intrusion management, all centralized in a monitoring center. A sensitive site needs to be protected on several levels: access protection, intruder sensors, CCTV, perimeter control… even drones. Our solution integrates all monitoring data and allows your teams to effectively monitor your sites.

CONTACTS:

ATOS
Rue Jean Jaurès BP 68
78340 LES CLAYES - FRANCE
Tel.: +33 (0)1 30 80 35 10
Web site: www.atos.net

Dan NIZARD
Atos Cybersecurity Sales director
Dan.nizard@atos.net

Business Line of Bertin Technologies (CNIM Group), Bertin IT designs and provides software solutions meeting the highest needs on the fields of cyber security, cyber intelligence and voice recognition.

Its offer covers the security of sensitive information systems and critical infrastructures, and the in-depth analysis of open source multimedia and multilingual data for detecting threats and enhancing situational awareness.
With its subsidiary Vecsys, specialized in voice technologies, Bertin IT also provides solutions and services dedicated to multilingual speech-to-text transcription of audio/video sources, the development of linguistic resources and embedded voice command.

PolyXene®, sensitive information systems & critical infrastructures high security software platform

CC-EAL 5 certified, PolyXene® relies on more than ten years of close cooperation between Bertin and the French arms procurement agency (DGA) on partitioning classified information and secured exchange of sensitive data issues.
PolyXene® natively integrates several security building blocks, including:

- partitioning of data and applications of different levels of sensitivity (e.g. public vs. restricted) on a single workstation (fixed or nomad) ;
- role based access control and strong authentication for limiting potential impact of an intrusion in case of a corrupted session ;
- data encryption for fighting against attacks using hidden files or rewriting on the fly.

WhiteN®, USB threats neutralizer

WhiteN® achieves high protection against attacks using removable media (USB peripherals, CD-Rom, smartphones, etc.) with sanitizing and file format verification, as well as whitelisting and filtering peripheral by classes which enables to block any unauthorized device (e.g. malicious devices of the kind of BadUSB). WhiteN® also has partitioning properties that makes it possible to confine the environment being accessed by the peripheral. Doing so, even though an attacker succeeds in spoofing an approved device, his possibilities to harm are limited to the corrupted machine.

MediaCentric®, multimedia multilingual open sources in-depth analysis platform

An all-in-one solution for anticipation and investigation, MediaCentric® covers a whole monitoring process including the massive collection of multimedia multilingual (Chinese, Russian, Arabic, Spanish, English…) contents from open sources (Web, TV, Radio), the in-depth analysis, the dynamic visualization and the edition of reports for disseminating information.
The French Armed Forces had acquired two of these platforms for cyber intelligence needs and critical issues.

CONTACTS:

BERTIN IT
10 bis avenue Ampère
78180 Montigny-le-Bretonneux-FRANCE
Tel.: +33 (0) 1 39 30 60 58
Website: www.bertin-it.com

Stéphanie BLANCHET
Communication / Marketing Manager
stephanie.blanchet@bertin.fr

Brainwave is a leader in IT fraud, data leakage and cyber espionage risk analysis and mitigation.

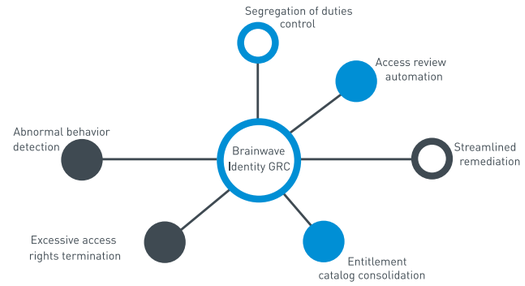
Excessive access rights, removal of access privileges, segregation of duties are the top 3 problems found when external audits are made and are the cause of most fraud and data leaks.
Brainwave addresses these issues with an innovative analytics solution. Brainwave IdentityGRC allows mapping and continuous monitoring of access rights to applications, structured and unstructured data, on premise or in the cloud.

The Brainwave solution simplifies Identity Governance. Installed on top of legacy provisioning systems or as a standalone application, Brainwave enables your organization to achieve sustainable compliance and empowers your business people with the tools needed to effectively manage their assets security.

Brainwave brings you 360° snapshots of your users, their granular permissions and their activities. Its patented analytics engine automatically highlights all abnormal situations, thus helping you reduce fraud and data leakage risks.

- Analyze applications' permissions, file shares and physical access
- Maintain a full history of the people and their access rights
- Comes up with more than 200 analytics and reports out-of-the-box
- Provides production ready remediation and access review workflows
- Installed in days
- Connector less

By using Brainwave, our clients significantly reduce their risks of fraud and data leaks by ensuring that access rights to sensitive information are managed on a need-to-have basis.
Brainwave has been named Gartner Cool Vendor 2013 and is distributed through a network of consulting partners across Europe, Africa, Canada and the US.



CONTACTS:

BRAINWAVE
38 - 42 rue Gallieni
92600 ASNIERES-SUR-SEINE
FRANCE
Tel.: +33 (0)1 84 19 04 11
www.identityanalyticsintelligence.com

Cyril GOLLAIN
CEO
Mobile: +33 (0)6 13 78 52 04
cyril.gollain@brainwave.fr

COFELY INEO
GDF SUEZ

As a major player in electrical engineering, information and communication systems, and related services, Cofely Ineo provides its public and private customers with overall solutions from design to operational and security maintenance.
Cofely Ineo brings solutions to secure infrastructure related to industrial systems, information systems, and mobile network.

Ensuring data security in cyberspace

Our offers are built from proven and qualified technology used by the French Authorities. They bring protection for data in terms of confidentiality, integrity, availability and traceability.
Our solutions provide this security level for both data storage and data transport.

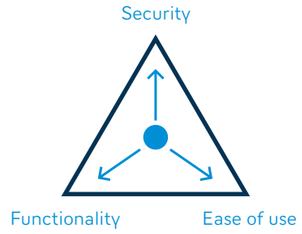
Data storage securization
- On server
- On smartphone, mobile terminal
- Inside public or private cloud

Communication network securization
- Fixed communication network
- Wireless network

Insure the security of the infrastructure

In order to respect defense in depth principle, our security experts design secure architectures. Those architectures are consistent with the state of the art, from design to secure maintenance.

Our solutions are designed in order to have the right balance between:
- Functionality
- Ease of use
- Security



In addition, the knowledge and experience of Cofely Ineo in signals intelligence, allow us to propose solutions for protection of electronic and computer systems against compromising emanations.

Cybersecurity services

Our teams of experts in cybersecurity are able to provide services in organizational, architecture and system audits.
To ensure systems maintenance in secure conditions, we are also able to provide vulnerability monitoring and impact analysis.

CONTACTS:

COFELY INEO
1 place des degrès
92059 Paris La Défense Cedex - FRANCE
Tel.: +33 (0)1 57 60 42 00
Fax: +33 (0)1 57 60 42 01
Web site: www.cofelyineo-gdfsuez.com

Josyane LOURDIN
Ineo Cyber Sécurité
Mobile: +33 (0)6 84 61 67 08
josyane.lourdin@cofelyineo-gdfsuez.com

denyall
NEXT GENERATION APPLICATION SECURITY

DenyAll is a European software vendor, an expert in Next Generation Application Security. Building on 15 years of experience securing web applications and services, the company keeps on innovating to meet the needs of organizations of all sizes, worldwide.

To fight against modern attacks targeting your IT infrastructure, an efficient strategy calls for reducing your attack surface, by proactively managing IT vulnerabilities, and filtering incoming Web traffic to stop application-layer attacks from accessing your critical back-end servers. The purpose of DenyAll's Next Generation Application Security products is to help you detect security weaknesses, protect the application layer, safely connect users and manage the process, with a view to improving your security posture over time :

Vulnerability Management

DenyAll's vulnerability scanners help organizations detect the network, system and application layer vulnerabilities which can potentially be exploited by hackers to gain access and steal your data. Based on a shared platform, they meet the needs of auditors, IT and security teams alike.

Web Application Security

DenyAll's web application firewalls (WAF) protect any application accessible via a web browser or mobile app. That include Internet-facing transactional web sites (e-Banking, e-Commerce, e-Government, etc) , messaging and collaborative portals, critical databases and web services based communications.

Web Access Management

DenyAll's Web Access Manager (WAM) helps safely connect users to your web applications, making security easier for them (Web Single Sign On), while strengthening authentication for protected applications. DenyAll Client Shield makes sure the browsers connecting to your applications are not the vectors of data leakages.

Security Management

DenyAll products provide the ability to centrally manage controls, wherever and whenever they need to be deployed, and to make sense of the data they log, with centralized dashboarding and reporting based on key security indicators. This is essential to understanding what happened, after the fact, and improving over time.

Certifications

DenyAll is very proud to be one of the companies awarded the 'France Cybersecurity' label in January 2015.The French government agency for IT security (ANSSI), has issued its 'Certification de Sécurité de Premier Niveau - CSPN' to both DenyAll rWeb and BeeWare i-Suite in June 2013 and September 2014, respectively. In the Gartner's first Magic Quadrant for WAFs, published in June 2014, DenyAll is very well positioned in terms of "completeness of vision", thanks to its innovation in security.

CONTACTS:

DENYALL
6 avenue de la Cristallerie
92310 SÈVRES - FRANCE
Tel.: +33 (0)1 46 20 96 00
Fax: +33 (0)1 46 20 96 02
Web site: www.denyall.com

Stéphane de Saint Albin
VP Marketing & Business Development
Tel.: +33 (0)1 46 20 96 21
sdesaintalbin@denyall.com

ercom

Cryptosmart solution prevents against all the threats mobile workers may encounter: **lost or stolen terminals, eavesdropping and intrusion on handsets on best-in-class Smartphones, Tablets and PC.**

Cryptosmart **secures mobile phones for all communications** (voice, data, mail, SMS) and on all networks (GPRS, EDGE, 3G, HSDPA, LTE™, Wi-Fi®, Satellite, etc).
We guarantee to our users the confidentiality of their data and voice exchanges as well as a user-friendly solution.
Cryptosmart includes a set of security software and a patented encryption technology embedded in a fully secured smartcard. Indeed, the Cryptosmart applet certified EAL4+ is enclosed in a EAL5+ smartcard. The Cryptosmart solution is certified French and NATO Restricted Product.
The solution secures all data flows (emails, Intranet/Internet accesses, business applications…) and enables both encrypted-clear and encrypted-encrypted voice communications.
Cryptosmart is already used by numerous governmental entities and sensitive corporations.

CRYPTOSMART

Strong security for mobile communications (voice and data) on best-in-class Smartphones and Tablets.

✓	**Security for mobile, fixed and satellite networks**
✓	**Security of data stored on Smartphones and Tablets**
✓	**Secure voice**
✓	**Secure SMS**
✓	**Mail & intranet security**
✓	**Secure internet access**
✓	**Strong authentification**
✓	**France & OTAN restricted**
✓	**Customer cryptographic independence**
✓	**Information system access control**

CONTACTS:

ERCOM
6 rue Dewoitine
Bâtiment Émeraude
78140, VÉLIZY-VILLACOUBLAY
FRANCE
Tel.: +33 (0)1 39 46 50 50
Web site: www.ercom.com
Email: contact@ercom.fr

ilex International

Ilex International is a software provider specialising in Identity & Access Management solutions (IAM).

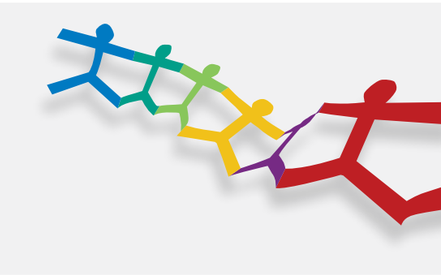
Provider to most of the blue chip companies, throughout the past 25 years, the company has developed proven expertise in both data access control and identity and rights management.

Ilex International's solutions are business-oriented and meet the requirements of all companies and organizations focused on the security of their information system, in France and worldwide.

Overtime Ilex International has built a strong and reliable network of specialised partners.
Whether they are market leaders or highly specialised consulting firms with strong expertise in IT security, they provide customers with complementary software or high level consulting and integration services. This allows Ilex International to offer, in addition to its IAM and CMS (Card Management System) product line, a large range of best of breed well integrated complementary solutions as well as appropriate local and global support throughout the world.

Ilex International's offering is centred on 4 products:
- **Sign&go:** Strong authentication, access control, global SSO (WAM and Enterprise SSO) and identity federation solution.
- **Meibo:** Identity and rights management, business workflows and user provisioning solution
- **Meibo People Pack :** A packaged solution for managing user's lifecycles and their rights within the organisation
- **IDen Park :** Deployment of authentication devices (smartcards, USB keys, badges) and management of their lifecycles

The success of identity and access management projects is based on the quality of the solutions as well as the ability to provide personalised and highly competent professional services. Ilex International makes it a priority to provide outstanding consulting, training, and support to their customers and partners and to ensure that their needs are properly met throughout the project life cycle.
The company is a founder member of the Hexatrust association.



Identity Management

Access Management

Authentication Device Management

CONTACTS:

ILEX INTERNATIONAL
51 boulevard Voltaire
92600 ASNIÈRES-SUR-SEINE
FRANCE
Tel.: +33 (0)1 46 88 03 40
Fax: +33 (0)1 46 88 03 41
Web site: www.ilex-international.com

Thierry BETTINI
Sales Director / Sales Department
thierry.bettini@ilex-international.com

OPENTRUST

OpenTrust is a leading provider of trusted identity-based solutions for protecting credentials, data and transactions. We are also an internationally recognized Certification Authority.

OpenTrust's two major product lines are available as a cloud service or under a software license:

- Trusted Identities, afeaturing strong authentication and certificate lifecycle management for any type of media or device (PC, smartphone, tablet, badge, token)

- Trusted Documents and Transactions, featuring digital signatures, confidentiality and proof management.

Every day, millions of people around the world use OpenTrust technologies with their corporate badges, their passports, when signing contracts, insurance policies, loans, rental agreements, and more, both on-line and in person.

OpenTrust operates in Europe, the Middle East and the USA through a network of local resellers.

Find out more at: www.opentrust.com

CONTACTS:

OPENTRUST
175 rue Jean-Jacques Rousseau
92138 ISSY-LES-MOULINEAUX Cedex
FRANCE
Tel.: +33 (0)1 55 64 22 00
Fax: +33 (0)1 55 64 22 01
Web site: www.opentrust.com
Caroline DROBINSKI
Marketing & Communication Manager
Mobile: +33 (0)6 89 72 69 41
caroline.drobinski@opentrust.com

PRIM'X TECHNOLOGIES

Prim'X is a developer of data encryption software for IT systems.

Prim'X Technologies develops encryption solutions to **effectively prohibit unauthorized access to sensitive information** whether local or remote, stored or exchanged.

The encryption solutions developed by Prim'X ensure encryption of data wherever they may be stored - internally on workstations or servers and externally on data-sharing servers – and encryption of information exchanges (e-mails, file attachments, portable devices, etc.).
Prim'X solutions guarantee **data access ubiquity** for users, in particular for roaming users by way of encryption applications dedicated to mobile terminals and/or their partners.
With these solutions it is possible to set up **cryptographic partitioning** of data between users, and to prohibit unauthorised access to data by third parties (technical personnel, Cloud service providers, etc.).
Prim'X is a driver of innovation and is continually developing its products so that they remain **perfectly suited to the needs of users**. Mobility and data security in the Cloud are the key concerns of the Prim'X development lab.

Certifications : Prim'X regularly gets its encryption software certified at **CC EAL3+** level and qualified at Standard level with the ANSSI (French national agency for information system security). **ZoneCentral, ZonePoint, Zed! and Cryhod** have all obtained these certifications. They have also received **NATO-Restricted and EU-Restricted** protection approval and "France Cybersecurity" labels for its products.

Main Prim'X encryption software:

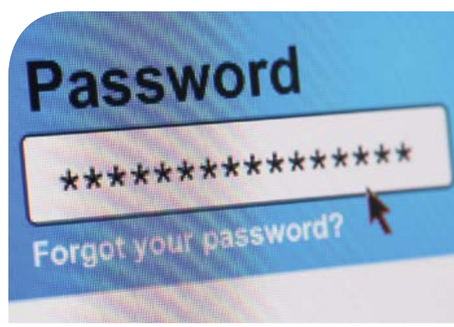
- ZoneCentral Protection of files stored on workstations, peripherals and servers

- Cryhod Protection of mobile workstations with pre-boot authentication and full-disk encryption

- ZonePoint Encryption of data shared on MS SharePoint and encrypted document securitye

- Zed! Encrypted containers for data archiving or email exchange (free reader available for all operating systems and platforms on http://www.zedencrypt.com)

- ZedMail Email confidentiality through end-to-end encryption with password or certificate authentication



CONTACTS:

PRIM'X TECHNOLOGIES
117 avenue Victor Hugo
92100 BOULOGNE BILLANCOURT
FRANCE
Tel.: +33 (0)1 77 72 64 82
Web site: www.primx.eu

Nicolas Bachelier
Sales Director
Mobile: +33 (0)6 60 40 38 41
nicolas.bachelier@primx.eu

RISK&CO SOLUTIONS

Launched in 1994, RISK&CO is a European engineering and risk intelligence group. Our areas of expertise are critical infrastructure projects and crisis areas.

Present in over 30 countries, we are leaders in all issues involving sovereign industries (energy, defence, telecommunications, …) and sensitive infrastructure projects in dangerous environments. Risk&Co, through its subsidiary Risk&Co Solutions carries out tasks of cyber security critical environments at both the SCADA systems and management information levels.

Our actions:

Cyber Security Consulting/Forensics

Integration of cyber security in complex projects:
- ✓ Assistance to formalize cyber security requirements
- ✓ Development of cyber security specifications
- ✓ Cyber security awareness sessions

Risk Assessments & basic engineering expertise:
- ✓ Initial identification of cyber security risks
- ✓ Early-stage design of security architectures
- ✓ Security review of network or application designs

On-call expertise throughout the lifecycle:
- ✓ Management awareness notes related to cyber security
- ✓ Technical notes for specific topics of expertise
- ✓ Design of use-cases of SIEM solutions

Technical audits & penetration testing

Penetration testing
- ✓ Methodology: Simulation of attacks against a given target in order to identify its vulnerabilities and highlight their impact, using the same tools and technics as real attackers.
- ✓ Typical targets: Internet access, Web applications, internal networks
- ✓ Deliverables: Audit report describing the methodology, the vulnerabilities identified, their consequences and the associated recommendations
- ✓ Variants: With or without user account or information on the target, depending on the scenario to evaluate

White-box reviews:
- ✓ Methodology: Comprehensive study through a review of the configuration, procedures, documents, or interviews
- ✓ Typical targets: Firewalls, high-criticality servers, admin practices
- ✓ Deliverables: Audit report describing the methodology, the vulnerabilities identified, their consequences and the associated recommendations

Security software engineering

Secure protocols:
- ✓ Design of secure communication protocols and cryptosystems
- ✓ Study of the security of existing protocols
- ✓ Securing of existing protocols

Design and development of security software
- ✓ Design and implementation of customized encryption applications
- ✓ Implementation of encryption and security libraries

Off-the-shelf products:
- ✓ SecureBooks: a secure document distribution solution for iPhone/iPad
- ✓ Simp: an instant messaging encryption solution
- ✓ Sereos: a secure mini-cloud infrastructure

CONTACTS:

RISK&CO
38, rue Jacques Ibert
CS 90519
92300 LEVALLOIS PERRET
FRANCE
Tel.: +33 (0)1 55 24 23 22
Email: info@riskeco.com
Web site: www.riskeco.com

Bruno DELAMOTTE
President

SURYS

Authentication and traceability of people, critical components and immaterial content

SURYS is a world leader in the development, production and marketing of optical and digital systems for protection of high security documents against fraud and counterfeiting.
SURYS covers various aspects of material and immaterial security. Three main activities predominate: authentication of identity documents, through our subsidiary Keesing Technologies which manages the world's largest database of ID document security features; fight against counterfeiting of components of sensitive equipment through **Optical Smart™** solutions; search of sensitive contents on the Internet thanks to **AdvestiSearch™ Authorities** products and services.

Authentication and Identification:

With **Documentchecker™** and **Authentiscan™**, SURYS offers solutions for identity document control, from a fixed or mobile unit, that determine unambiguously whether the identity document submitted by the applicant is genuine. This software compares the model tested with our Keesing References Systems™ database which contains over 20,000 images of more than 3,000 identity documents of nearly 200 countries and organizations.

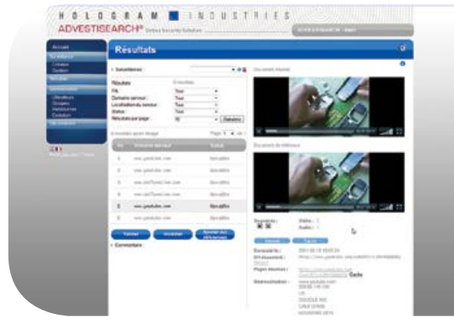
Security of Critical Components:

Anti-counterfeiting systems **Optokey™** and **Drop™** are dedicated to check the integrity of support and data linked to the physical components. They consist in labels applied to various objects guaranteeing their tamper evidence and traceability, automatically authenticated with specific Smartphone apps. Deployed on standard Smartphones, they can be used by non-trained people.

Data Collection:

AdvestiSearch™ Authorities product line, currently used by major actors like French Gendarmerie, allows to search for audiovisual and textual content by similarity on the Internet. From reference content, the system is able to identify low intensity signal, for instance an image or some seconds of a soundtrack embedded in a large YouTube video stream. They can be tracked and their source identified for diffusion control or investigation.

Automated Authentication and Traceability of sensitive components



Online sensitive data collection

Automated Authentication of ID documents

CONTACTS :

SURYS
(the new name for Hologram.Industries)
22 avenue de l'Europe,
77600 BUSSY SAINT GEORGES
FRANCE
Tél.: +33 (0)1 64 76 31 00
Site web: www.surys.com

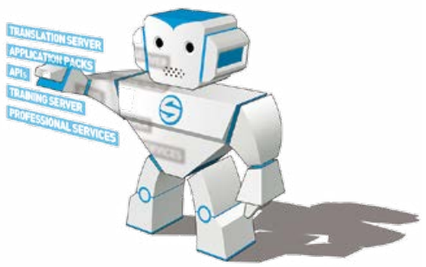
Corinne MURCIA GIUDICELLI
Director, Marketing,
Sales & Customer Relations
c.murcia@surys.com

SYSTRAN

Intelligent Language Technologies

In today's digital world, businesses or defense and security organizations are overwhelmed with massive amounts of data which tend to be more and more non-English. The lack of linguistic skills and expertise, especially in Middle Eastern languages, and the variety of sources and formats (text, audio, video, image) are the other major challenges they need to overcome in order to fight efficiently against cyber criminality.

For over four decades, SYSTRAN has been the market leader in language-translation products and solutions. With the ability to facilitate communication in 130+ language combinations, SYSTRAN is the leading choice of global companies, defense and security organizations or public agencies, enabling them to quickly understand and process large volumes of multilingual content.



Ensure information security in your translation processes

By providing a centralized translation server directly on site, SYSTRAN offers fully secure, real-time automated translation regardless of the document formats. All sensitive information stay secure because your data and translations never leave your network, thus preventing data leakage.

Quickly translate large volumes of content

SYSTRAN's high performance and scalable architecture delivers fast translations, allowing you more time to spot and analyze critical information.

Reduce translation costs

The use of automated language identification and automated machine translation dramatically reduces the need for human translation, therefore lowering costs.

Make your electronic investigations smarter

SYSTRAN's Linguistic Development Kit enables you to get all your multilingual Big Data in a searchable and manageable form. Taken separately, each module is an efficient tool for processing language, documents or names. Combining them, you benefit from powerful multilingual capabilities for data mining or semantic search solutions. The key linguistic libraries, listed below, are available in all the **45+ languages** supported by SYSTRAN.

- **Document Filtering**
- **Language Identification**
- **Segmentation and Tokenisation**
- **Language Normalisation**
- **Document Classification**
- **Named Entity Recognition**
- **Dictionary**
- **Morphological analysis**
- **Syntactic Analysis**
- **Transliteration**
- **Word Sense Disambiguation**

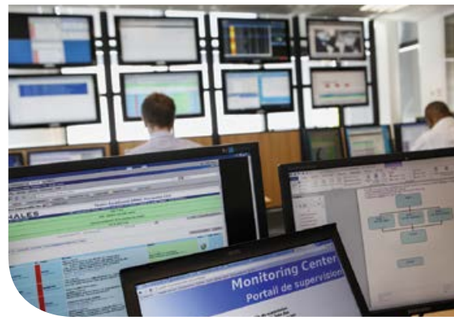
SYSTRAN language technologies let you utilize and analyze both structured and unstructured multilingual content, such as user-generated content, social media, Web content and more. To help you manage even more document formats, **OCR** (optical character recognition) and **ASR** technologies can easily be integrated with SYSTRAN.

CONTACTS:

SYSTRAN
5 rue Feydeau - 75005 PARIS - FRANCE
Tel.: +33 (0)1 44 82 49 00
Fax: +33 (0)1 44 82 49 01
Website: www.systransoft.com

Emmanuel TONNELIER
Senior Account Manager, EMEA
Defense & Security
Mobile: +33 (0)6 67 40 03 31
emmanuel.tonnelier@systrangroup.com

THALES



Thales is a global leader in cryptographic security products and solutions for critical government and defence infrastructure, satellite networks, enterprise customers and the financial services industry. Thales's unique positioning in the marketplace derives from its ability to address every link in the security chain and deliver end-to-end solutions.

As of January 2015, there were approximately three billion internet users in the world and more than 1.2 billion websites. The internet has grown exponentially and so have the number of cyberattacks. Information systems and the internet play such a prominent role in government and business — and in people's day-to-day lives — that they are critical to a country's economic performance and national security. Today, cybersecurity has become an existential challenge for governments, essential operators and businesses in every sector.

Thales expertise in cyberspace

With a presence throughout the entire security chain, Thales offers a comprehensive set of solutions and services ranging from security consulting, intrusion testing and architecture design to system certification and the development and lifecycle management of products and services.

Thales provides the IT solutions and human resources needed to protect information systems and to monitor, detect, analyse, visualise and counter all types of current and future cyberattacks, including virus attacks, disinformation, denial-of-service attacks, destabilisation, data destruction, defacement and theft.

Cybersecurity is an integral part of the Thales offering for the Aerospace, Transportation, Defence and Security sectors and is central to the company's role in the Defence-Security Continuum.

By choosing Thales, you benefit from:

- A team of 5,000 critical IT engineers with 1,500 experts in cybersecurity
- A partner with more than 40 years of experience protecting classified information up to the Top Secret level
- A global actor with products and solutions deployed in more than 50 countries
- A reliable service provider with experience operating and monitoring the critical information systems of over 100 customers

Our clients include:

- 19 of the 20 largest global banks
- 4 of the 5 largest oil companies
- 27 NATO country members

CONTACTS:

Critical Information Systems and Cybersecurity, Thales

www.thalesgroup.com/cic

THEGREENBOW

TheGreenBow is a French Cybersecurity Software company providing off-the-shelf data encryption solutions for personal computers and mobile platforms.

Located in Paris/France since 1998, TheGreenBow has acquired a unique skill set in building user friendly encryption tools combining the highest level of security and unequalled ease-of-use. TheGreenBow security solutions are appreciated by a large community of users worldwide and are renowned for their solid implementation, their reliability and for their ergonomic user interfaces. TheGreenBow provides Software solutions for secure Network communications (VPN) and email privacy (email encryption). With over one million licenses distributed worldwide, 70% of sales in export, over 15 years of experience in building cryptographic Software for privacy protection in a B2B market and the recent achievement of Common Criteria EAL3+ Certification, TheGreenBow is a leading provider of trusted and scalable security solutions suitable for SMEs, large accounts, Critical Infrastructures, Government and civil administrations, … TheGreenBow is a founding member of HexaTrust, member of the competitive cluster « Pôle Systematic » and contributor to the Government Plan for strategic development in key areas (Nouvelle France Industrielle).

VPN Client

Reliable and secure remote connections

Multi-protocol support (IPsec & TLS), compatible with virtually all VPN Gateway, providing reliable fast and highly secure VPN connections over any type of Network, TheGreenBow VPN Client is the ideal solution for secure remote Network access.

Premium VPN Client

Scalable, and designed for seamless integration with corporate IT infrastructures

Compatible with any PKI, simple and quick integration with existing IT infrastructures, built-in facilities for large-scale deployment - TheGreenBow Premium VPN Client is designed for integration within large corporate Networks (government administrations, critical infrastructures, and large enterprises).

Certified VPN Client

Certified and audited government grade VPN

TheGreenBow certified VPN client is the first VPN client worldwide to achieve Common Criteria EAL3+ certification as well as NATO end EU restricted qualification.

Android VPN Client

Secure VPN for Tablets and Smartphones

TheGreenBow Android VPN Client extends the range of professional solutions provided by TheGreenBow for secure remote connections.

CryptoMailer

Universal email privacy

True end-to-end email encryption, making email privacy a user-friendly and painless experience. Integrated with major email clients (Outlook, Thunderbird, Livemail, ..) and compatible with virtually any existing email system and Webmail and any operating system. Truly revolutionary.

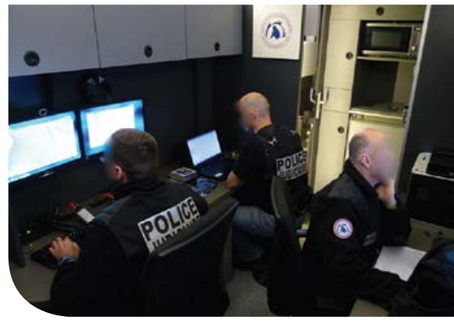
CONTACTS:

THEGREENBOW
28 rue de Caumartin
75009 PARIS - FRANCE
Tel.: +33 (0)1 43 12 39 37
Fax: +33 (0)1 43 12 55 44
Web site: www.thegreenbow.com

Sales department
sales@thegreenbow.com

TRACIP
Forensics Services & Technologies

With more than 20 years of experience, TRACIP is a french company that pioneered Data Recovery and Computer Forensics Services in France.



Working daily on cases, TRACIP is the leading French Data Recovery & Digital Investigation Laboratory and a leading provider in Consulting, Equipment & Training for Corporations and Government Agencies.

Our customers are large Corporations, Law Enforcement and Government Agencies, Regulation Authorities… which trust TRACIP to support them in their fight against Cyber criminality.

We offer services, equipment and training to Law Enforcement Agencies and Corporations, including:

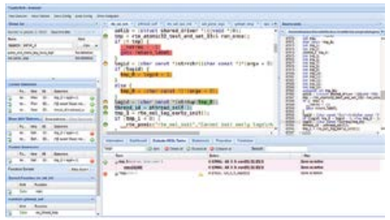
- Creation of Customized Turnkey Digital Forensic and Data Recovery Laboratories
- Consulting for in-house Digital Investigation
- Data Recovery, Computer Forensic and Cybersecurity Trainings
- Mobil'IT® : TRACIP is the designer and manufacturer of the first forensic mobile laboratory with Data Recovery and Digital Forensic capabilities built for field investigation

CONTACTS:

TRACIP
6 rue Robert Schuman
ZA Le Breuil
54850 MESSEIN - FRANCE
Tel.: +33 (0)3 83 50 54 63
Fax: +33 (0)9 70 06 31 45
Email: contact@tracip.fr
Web site: www.tracip.fr

TRUSTINSOFT

- Telecom
- Energy
- Space
- Defence
- Railways
- Aeronautics



TrustInSoft is the only software vendor able to assess safety and security of software without the need to change software development process.

TrustInSoft sells tools and services to analyze source code. TrustInSoft unique value proposal is to bring guarantees on the behavior of software. TrustInSoft solutions are currently in use for software designers or integrators in the following domains: aeronautics, military, energy, telecom, space, railways.

TrustInSoft proposes the following tools and services:

TrustInSoft Analyzer, the award winning software analysis tools allowing to mathematically guarantee the conformity to a specification or the absence of flaws in software.

TrustInSoft Advances software audits, a service in which TrustInSoft experts uses TrustInSoft Analyzer on the customer's software. This service enables to get guarantees on the analyzed software.

TrustInSoft Expertise, a service of expertise to help customers use and deploy TrustInSoft Analyzer. It consists of training sessions, methodological help or event design of dedicated TrustInSoft Analyzer plugins.

CONTACTS:

TRUSTINSOFT
86 rue de Paris
91400 ORSAY - FRANCE
Tel.: +33 (0)9 70 44 75 87
Web site: www.trust-in-soft.com

Fabrice DEREPAS
CEO
Mobile: +33 (0)6 51 70 36 77
fabrice.derepas@trust-in-soft.com

VADE-RETRO
NEXT-GEN EMAIL FILTERING

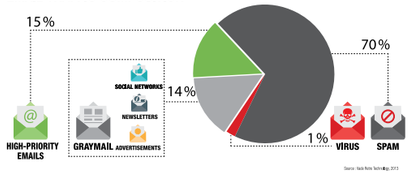
Always more low-priority emails…
Take back control over your emails.

The issue is no longer spam, which is now well regulated by most anti-spam solutions on the market.

The problem has shifted to low-priority emails, called graymail.
The proportion that graymail occupies in the global mail volume has reached 50% in professional mailboxes. There is of course a solution to the problem, but it is tedious – deleting these emails every day and unsubscribing from them manually.

Advertisement emails and other notifications are not spam.
However, 82% of users see them as a nuisance and have indicated their dissatisfaction with their email filter solutions (Gartner Magic Quadrant 2013).

EMAIL TRAFFIC COMPOSITION



Spare your employees the daily graymail cleanup. Vade Retro Technology' filter solution does not compromise on security, protecting you from spam phishing and viruses thanks to an innovative heuristic technology.
Associating automatic classification of low-priority emails with safe unsubscriptior from newsletters in 1 click, the Vade Retro solution offers a global, simple and effective response to your expectations: more productivity and control over your mail.

The heuristic filter: the security layer.
Fast and accurate, email scans do not require connections to external services. The filter is operational immediately after installation and is effective against waves of targeted attacks.

Automatic graymail classification.
Emails are sorted by their nature: person-to-person, advertisement, newsletter, social network notification, etc. We classify your emails according to your filter policy and strategy.

Safe unsubscribe in 1 click. The process takes place in real time and delivers results in 1.4 seconds with a success rate of 84%.
The procedure is identified during the filtering phase and supports all unsubscription methods

The solution adapts to your needs and infrastructure.
The solution runs independently from your mail client. Available through a virtual or physical gateway, a cloud service and a development kit SDK.

CONTACTS:

VADE RETRO TECHNOLOGY
3 av Antoine Pinay,
Parc d'activités des 4 vents
59510 HEM - FRANCE
Tel.: +33 (0)3 28 32 80 44
Web site: www.vade-retro.com

Grégoire LEPOUTRE
VP Sales & Strategic Partnerships
commercial@vade-retro.com

Traceability

Privileged Account Session Management

Password Management

CONTACTS:

WALLIX
250 bis rue du Faubourg-Saint-Honoré
75008 PARIS - FRANCE
Tel.: +33 (0)1 70 36 37 51
Fax: +33 (0)1 43 87 68 38
Web site: www.wallix.com

François LACAS
Marketing Director
Mobile: +33 (0)6 63 65 72 36
flacas@wallix.com

WALLIX
TRACE, AUDIT & TRUST

At WALLIX our mission is empowering your organisation to confidently give the right people access to the right IT systems. Our approach to security isn't just blocking access but giving you the freedom and visibility to keep your staff, service providers and contractors working securely and effectively.

WALLIX engineers software solutions that give our customers all over the world a better way to manage and secure access to IT infrastructure for privileged users. Creating a single gateway with single sign-on for access by members of internal IT teams or third party service providers.

Access rights and passwords to servers, appliances and other devices can all be handled in a single console, helping to manage IT team turnover and ensure that critical servers are only accessed by the people you've approved. And we take you beyond event logging by letting you monitor and capture session activity in real-time.

WALLIX AdminBastion (WAB) is developed and maintained by our experienced in-house team. And we keep usability at the heart of our philosophy. The WAB is engineered as a non-intrusive and agentless technology making it simple for you to configure, operate and administer day to day. No software is required on either the client or target devices.

We're growing fast, supported by a global network of certified partners and value-added resellers across EMEA, CIS, APAC and North America. Our honesty and commitment to supporting our customers is why more than 200 organisations worldwide choose WALLIX. We offer the best solution and value from a company that's easy to work with.

Wallix AdminBastion is a solution to help your organisation manage and monitor users who have privileged access to IT infrastructure, including servers, business applications and other devices.

AdminBastion is able to monitor activity on systems of any operating system in real time, give immediate access to video recordings of these sessions as well as comprehensive auditing to help you meet compliance requirements.

Our solution creates a single gateway with single sign-on for access by members of internal IT teams or third party service providers. Access rights and passwords to servers and other devices can be handled in a single console helping to manage IT team turnover and ensure that critical servers cannot be accessed by individuals no longer authorised to do so.
It provides records and audit trails to demonstrate optimised compliance with applicable standards (ISO2700, PCI DSS, etc.).

AIR-LYNX

Atos

bertin

BRAINWAVE

COFELY INEO
GDF SUEZ

denyall
NEXT GENERATION APPLICATION SECURITY

ejcom

ilex
International

OPENTRUST

PRIM'X
TECHNOLOGIES

RISK & CO
SOLUTIONS

SURYS

SYSTRAN

THALES

THEGREENBOW

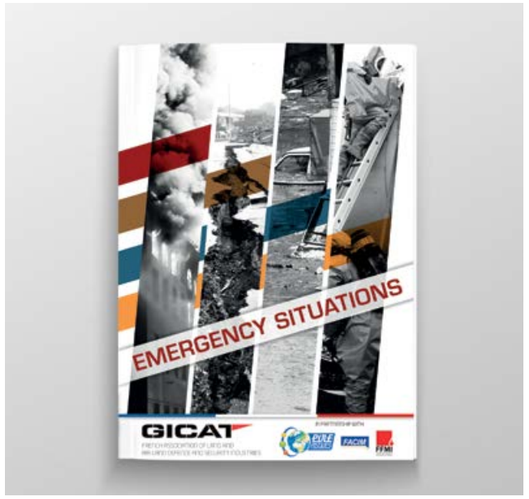
TRACIP
Forensics Services & Technologies

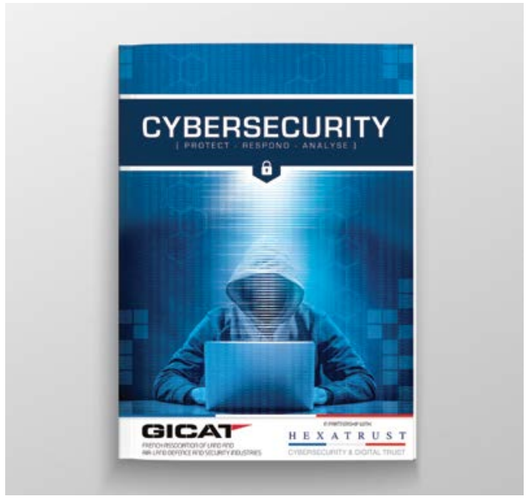
TRUSTINSOFT

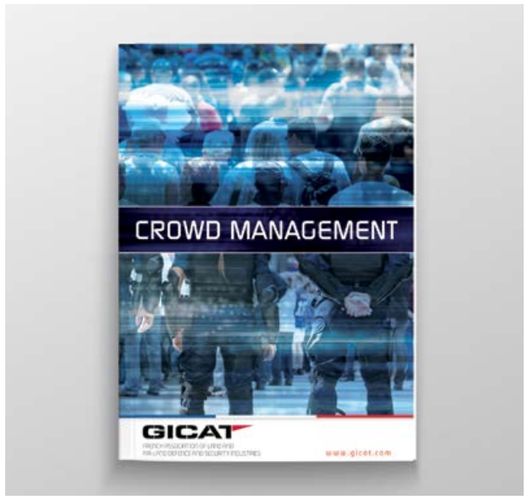
VADE-RETRO
NEXT-GEN EMAIL FILTERING

WALLIX
TRACE, AUDIT & TRUST

SECURITY OFFER







GICAT

GICAT (Groupement Professionnel des Industries Françaises de Défense et Sécurité Terrestres et Aéroterrestres, French land defence and security industry association) represents 200 companies including industrial contractors, system manufacturers, integrators, and equipment manufacturers covering a broad spectrum of industrial, research, service and consulting activities. GICAT promotes the interests of the profession and works actively to support its members, particularly SMEs, in the international arena. The association also develops important ties with institutional and private players in the French security sector. GICAT also offers a number of exportation support services for its members, such as watch for international calls to tender, country information folders, Business to Business meetings, visits with delegations and authorities, participation in specialised trade fairs and thematic seminars.

GICAT

French land defence and
security industry association

3 Avenue Hoche
75008 Paris - FRANCE

Tel.: +33 (0)1 44 14 58 20

www.gicat.com

IN PARTNERSHIP WITH:

HEXATRUST

CYBERSECURITY & DIGITAL TRUST

250 bis rue du Faubourg-Saint-Honoré
75008 Paris - FRANCE

Tel.: +33 (0)1 70 36 37 66

www.hexatrust.com

Design and Production: Agence Kervert